

# ELECTRONIC INFORMATION DISCLOSURE STATEMENT

Electronic Version v18

Stylesheet Version v18.0

## Title of Invention

MANAGING A SECURE ENVIRONMENT USING A CHIPSET IN  
ISOLAQTED EXECUTION MODE

Application Number : 09/668408



Confirmation Number: 2377

First Named Applicant: Carl Ellison

Attorney Docket Number: P8628X

Art Unit: 2131

Examiner: Taghi T Arani

Search string: ( 3996449 or 4430709 or 4621318 or 5944821 or 5956408 or 6044478 or 6175924 or 6327652 or 6615278 or 6678825 or 20010027511 or 20020007456 or 20020023032 or 20020147916 or 20020166061 or 20020169717 or 20030074548 or 20030115453 or 20030126442 or 20030126453 or 20030159056 or 20030188179 or 20030196085 or 20040117539 ).pn

## US Patent Documents

Note: Applicant is not required to submit a paper copy of cited US Patent Documents

init	Cite.No.	Patent No.	Date	Patentee	Kind	Class	Subclass
<i>J.A</i>	1	3996449	1976-12-07	ATTANASIO			
<i>J.A</i>	2	4430709	1984-02-07	SCHLEUPEN			
	3	4621318	1986-11-04	MAEDA			
	4	5944821	1999-08-31	ANGELO			
	5	5956408	1999-09-21	ARNOLD			
	6	6044478	2000-03-28	GREEN			
	7	6175924	2001-01-16	ARNOLD			
	8	6327652	2001-12-04	ENGLAND			
	9	6615278	2003-09-02	CURTIS			
<i>J.A</i>	10	6678825	2004-01-13	ELLISON			

## US Published Applications

Note: Applicant is not required to submit a paper copy of cited US Published Applications

init	Cite.No.	Pub. No.	Date	Applicant	Kind	Class	Subclass
<i>J.A</i>	1	20010027511	2001-10-04	WAKABAYASHI			
<i>J.A</i>	2	20020007456	2002-01-17	PEINADO			
<i>J.A</i>	3	20020023032	2002-02-21	PEARSON			
<i>J.A</i>	4	20020147916	2002-10-10	STRONGIN			



<i>TA</i>	5	20020166061	2002-11-07	FALIK		<i>/</i>	
<i>TA</i>	6	20020169717	2002-11-14	CHALLENGER		<i>/</i>	
	7	20030074548	2003-04-17	CROMER		<i>/</i>	
	8	20030115453	2003-06-19	GRAWROCK			
	9	20030126442	2003-07-03	GLEW		<i>/</i>	
	10	20030126453	2003-07-03	GLEW			
	11	20030159056	2003-08-21	CROMER		<i>/</i>	
	12	20030188179	2003-10-02	CHALLENGER		<i>/</i>	
	13	20030196085	2003-10-16	LAMPSON		<i>/</i>	
<i>TA</i>	14	20040117539	2004-06-17	BENNETT			

Signature

*Taghi J. Arami*

*8/16/05*

Examiner Name	Date

09/668,408

Reference No.	Application Serial No.	Patent No.	Title
J.A. 1	09/672,603		Controlling Accesses To Isolated Memory Using A Memory Controller For Isolated Execution
J.A. 2	09/822,986		Checking File Integrity Using Signature Generated In Isolated Execution
J.A. 3	09/538,951		Platform And Method For Issuing And Certifying A Hardware-Protected Attestation Key
J.A. 4	09/539,344		Managing A Secure Platform Using A Hierarchical Executive Architecture In Isolated Execution Mode
J.A. 5	09/668,585		Managing A Secure Platform Using A Hierarchical Executive Architecture In Isolated Execution Mode
J.A. 6	09/541,108		Platform And Method For Remote Attestation Of A Platform
J.A. 7	09/540,612		Platform And Method For Generating And Utilizing A Protected Audit Log
J.A. 8	09/540,946		Protecting Software Environment In Isolated Execution
J.A. 9	09/668,610		Protecting Software Environment In Isolated Execution
J.A. 10	09/538,954		Generating Isolated Bus Cycles For Isolated Execution
J.A. 11	09/539,348	6,760,441	Generating A Key Hierarchy For Use In An Isolated Execution Environment
J.A. 12	09/541,477	6,507,904	Isolated Instructions For Isolated Execution
J.A. 13	09/540,611		Managing Accesses In A Processor For Isolated Execution
J.A. 14	09/540,613		Managing A Secure Environment Using A Chipset In Isolated Execution Mode
J.A. 15	09/668,408		Managing A Secure Environment Using A Chipset In Isolated Execution Mode
J.A. 16	09/541,667		Attestation Key Memory Device And Bus
J.A. 17	09/672,602		Attestation Key Memory Device And Bus
J.A. 18	09/618,738	6,678,825	Controlling Access To Multiple Isolated Memories In An Isolated Execution Environment
J.A. 19	09/618,489	6,633,963	Controlling Access To Multiple Memory Zones In An Isolated Execution Environment
J.A. 20	10/683,542		Controlling Access To Multiple Memory Zones In An Isolated Execution Environment
J.A. 21	09/618,659		Resetting A Processor In An Isolated Execution Environment
J.A. 22	09/751,586		Resetting A Processor In An Isolated Execution Environment